Sprint
Together with NEXTEL

Sprint Nextel
Mailstop VARESP0403-A4134
2001 Edmund Halley Drive
Reston, Virginia 20191
(703) 433-4605

Anthony Alessi
Senior Counsel

Electronic Filing via ECFS

March 1, 2008

Marlene H. Dortch
Office of the Secretary
Federal Communications Commission
445 12th Street, SW, Suite TW-A325
Washington, DC 20554

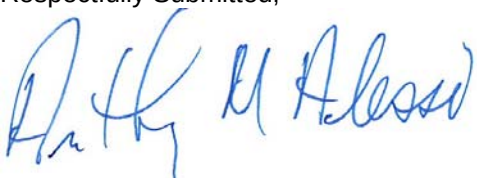
Re: **Annual CPNI Compliance Certification, EB Docket No. 06-36**

Dear Secretary Dortch:

Attached, for filing in EB Docket No. 06-36, is the Annual 47 C.F.R. § 64.2009(e) CPNI Compliance Certification and accompanying statement of Sprint Nextel Corporation.

If there are questions regarding this filing, please contact the undersigned. Thank you for your assistance.

Respectfully Submitted,



Anthony Alessi
Senior Counsel
Sprint Nextel Corporation

cc: Federal Communications Commission
Enforcement Bureau, Telecommunications Consumers Division
445 12th Street, SW
Washington, DC 20554
(2 copies via courier)

cc: Best Copy and Printing
(via email to FCC@BCPIWEB.COM)

cc: Marcy Greene
(via email to Marcy.Greene@fcc.gov)

Sprint Nextel
Mailstop VARESP0403-A4134
2001 Edmund Halley Drive
Reston, Virginia 20191

Kent Y. Nakamura
Vice President and Chief Privacy Officer

Annual 47 C.F.R. § 64.2009(e) CPNI Certification
EB Docket 06-36

Annual 64.2009(e) CPNI Certification for Sprint Nextel Corporation

Date Filed: March 1, 2008

Name of company covered by this certification: Sprint Nextel Corporation

Form 499 Filer ID:

804636 – Sprint Communications Company lP
817198 – ASC Telecom, Inc
804639 – US Telecom, Inc.
811754 – Sprint Spectrum, LP
818104 – SprintCom, Inc.
812437 – Sprint Telephony PCS, LP
819060 – Phillie Co, LP
811156 – American PCS Communications
822116 – Nextel Communications-Consolidated
819224 – Nextel Partners, Inc.

Name of Signatory: Kent Y. Nakamura

Title of signatory: Vice Present and Chief Privacy Officer

SPRINT NEXTEL CORPORATION
2007 CPNI COMPLIANCE CERTIFICATE AND STATEMENT

I, Kent Y. Nakamura, certify that I am an officer of Sprint Nextel Corporation, and that I have personal knowledge that the company has established operating procedures that are adequate to ensure compliance with the Commission's CPNI rules (*see* 47 C.F.R. § 64.2001 *et seq*).

Attached to this certification is an accompanying statement explaining how the company's operating procedures ensure compliance with the requirements of section 64.2001 *et seq.* of the Commission's rules. The statement details what actions the company has taken against data brokers within the past year. Moreover it provides a summary of the customer complaints that the company has received in the past year concerning the unauthorized access to CPNI.

Executed on March 1, 2008.

Kent Nakamura
Vice President & Chief Privacy Officer
Sprint Nextel Corporation

SPRINT NEXTEL CORPORATION
ATTACHMENT A
2007 CPNI Compliance Statement of Operating Procedures

The following statement explains the operating procedures established by Sprint Nextel Corporation ("Sprint Nextel" or "Company") to ensure that it is in compliance with the Federal Communications Commission's CPNI rules. Sprint Nextel refers to all Sprint Nextel Corporation's operating entities and divisions, including those referred to as Sprint Nextel, Sprint, Nextel, Boost[1] or Xohm[2]. Sprint Nextel focused this year on enhancing its customer authentication and notification procedures to comply with new CPNI rules, converting its wireless customers to its new Unified Billing Platform (UBP), improving several CPNI processes to ensure optimization of its CPNI compliance regime and establishing a CPNI complaint reporting process that complies with the new FCC CPNI rules. Sprint Nextel's Office of Privacy, along with several business units, continues to monitor Sprint Nextel's systems and processes applicable to CPNI. As such, Sprint Nextel will continue to update CPNI training; review, and adjust where necessary its customer authentication, information-security, and notification procedures; and strengthen the Company's administrative, physical and technical safeguards.

Safeguards

Sprint Nextel employs administrative, physical and technical safeguards that are designed to protect CPNI from unauthorized access, use or disclosure.

Sprint Nextel limits CPNI access to employees, independent contractors and joint venture partners consistent with their job functions. If access is required, they must first obtain approval through established administrative processes. Once approval is granted, user IDs and passcodes are issued. Access credentials are governed by Sprint Nextel's Corporate Security policies, which meet industry standard requirements for passcode management for information technology networks, applications and databases.

When disclosing CPNI to independent contractors or joint venture partners, Sprint Nextel enters into agreements with strict privacy and confidentiality provisions that require third parties to maintain confidentiality, protect the information, and comply with the law. Sprint Nextel's Office of Privacy continually reviews Sprint Nextel's standard privacy-related terms and conditions to ensure that those provisions adequately safeguard all customer information. In negotiating and renewing its contracts Sprint Nextel has required independent contractors and joint venture partners with which it shares CPNI to safeguard this information in a manner that is consistent with the FCC's rules. Specifically, these contract terms require third parties with access to CPNI to have appropriate CPNI protections to ensure its ongoing confidentiality. Such provisions require securing all Sprint Nextel data; limiting access to persons who have a need-to-know such information in connection with the performance of the contract; ensuring all persons with access are bound by specified confidentiality obligations; and restricting the use of CPNI solely to the performance of the contract.

[1] Boost Mobile, LLC ("Boost") is a subsidiary of Sprint Nextel Corporation and offers a lifestyle-based youth brand presently focused on offering premium communications products and services.

[2] Xohm is a new business division of Sprint Nextel, with a mission to develop a better kind of wireless broadband experience. Xohm did not offer any services relevant to CPNI in 2007.

SPRINT NEXTEL CORPORATION
ATTACHMENT A
2007 CPNI Compliance Statement of Operating Procedures

Review and Recordkeeping for CPNI Marketing Use and Sharing

Sprint Nextel uses a marketing campaign management system for review, approval and record-keeping for outbound marketing campaigns that involve the use or sharing of CPNI. The standard process requires the requestor, who is internal to Sprint, to complete a form that describes the campaign and indicates whether CPNI would be shared and/or used as selection criteria for the campaign. Once the requestor has completed the form, it is submitted for review to determine whether the activity entails the use or sharing of CPNI consistent with the CPNI rules. This process ensures that Sprint Nextel does not use the CPNI in way that violates the CPNI rules. Records of all the foregoing activities are maintained, as required by the FCC's CPNI rules.

CPNI Notice and Consent Process

Sprint Nextel uses CPNI to provide customers with the services to which they subscribe. Effective May 2007, Sprint Nextel does not access, use or disclose CPNI for marketing services to which the customer does not already subscribe (cross-marketing). If CPNI is used for cross-marketing purposes, Sprint Nextel will obtain the appropriate consent as required by the CPNI rules. As such, Sprint Nextel ceased sending CPNI opt-out notices. Prior to May 2007, Sprint Nextel provided all new customers with a CPNI opt-out notice and sent refresher notices to existing customers every two years.

To the extent Sprint Nextel provides notice or obtains consent for access, use or disclosure of CPNI, CPNI records are maintained through a variety of systems and processes. This allows employees to determine the status of a customer's CPNI approval prior to any access, use or disclosure of CPNI that would require customer consent pursuant to the FCC's rules.

Sprint Nextel has never provided Boost Mobile customers with a CPNI opt-out notice because Boost does not use its customers' CPNI to cross-market other services in the manner contemplated under 47 CFR § 64.2008, thus making such notification unnecessary.

Sprint Nextel also has not accessed, used or disclosed CPNI for marketing of non-communications related products or services and thus has not obtained customer opt-in consent for such use or disclosure.

Training and Disciplinary Process

Consistent with Sprint Nextel's commitment to preserving customers' privacy, the Company has implemented a variety of training programs for its employees and contractors. The training explains how Sprint Nextel employees and contractors must access, use, store, disclose and secure CPNI to ensure compliance with the FCC's rules and Company policies.

Sprint Nextel also maintains a disciplinary process as part of the Company procedures which address CPNI compliance. Sprint Nextel security personnel investigate instances of potential improper access or disclosure of CPNI by employees. If the investigation indicates a violation has occurred, disciplinary action, up to and including termination, is taken.

SPRINT NEXTEL CORPORATION
ATTACHMENT A
2007 CPNI Compliance Statement of Operating Procedures

Authentication

During 2007 Sprint Nextel began converting its wireless customers to its new UBP. The UBP consolidates all Sprint Nextel wireless customers onto one billing platform. Most significantly, it delivers systematic features that substantially enhance customer authentication and security. Although the UBP project was underway before the FCC released its most recent *CPNI Report and Order*[3] in April of 2007, Sprint Nextel quickly developed and installed complex technical CPNI solutions within the context of the ongoing deployment of the UBP—a process that otherwise would have taken no less than 10 months to develop on a regular deployment schedule following the completion of all UBP software releases.

Within UBP, Sprint Nextel wireless customers establish a Personal Identification Number (PIN) that is required for account access to sensitive customer information. In the event a UBP customer cannot recall his/her PIN, the UBP allows customers to pre-select a security question and to provide an answer to that question. UBP customers who do not have a PIN are authenticated using a passcode from a previous billing system if one existed or by several other means, such as through secure third-party verification services or by visiting a retail location and providing a valid government issued photo ID. Where appropriate, Sprint Nextel may work directly with a business customer through a dedicated representative to establish an authentication regime that works best for that customer. As provided by the new CPNI rules, UBP customers are not authenticated using readily available biographical information or account information for access to call detail records over the telephone or when establishing or changing their PIN.

Sprint Nextel wireless customers who wish to obtain their call detail information have several options. If contacting Sprint Nextel by telephone with their PIN, Sprint Nextel will send call-detail records to an address designated by the customer at that time. If the customer does not have a PIN, Sprint Nextel will send the call detail records to the customer's "address of record," as defined by the new CPNI rules.[4] Customers with a valid, government issued photo-ID also may visit a Sprint Nextel retail store to establish or change his/her account PIN or to access call detail records.

As explained in its Waiver Petition,[5] Sprint Nextel migrated a majority of wireless customers to the UBP. Because of its reliance on technical solutions, however, Sprint Nextel did not complete the unique and complex migration by the effective date of the new CPNI rules. To date, Sprint Nextel continues to carefully migrate wireless customers in a way that minimizes any adverse impacts to the customer experience. For wireless customers not yet migrated Sprint Nextel continues to authenticate using pre-UBP systems and processes.

---

[3] *Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information; IP-Enabled Services*, Report and Order and Further Notice of Proposed Rulemaking, 22 FCC Rcd. 6927 (2007) ("*CPNI Report and Order*").

[4] *Id.* at ¶13 n.46; 47 C.F.R. § 2003(b).

[5] In the Matter of Implementation of the Telecommunications Act of 1996, *Petition for Limited Waiver*, CC Docket 96-115 (filed December 3, 2007) ("Waiver Petition").

For UBP wireless customers who wish to access their account online, Sprint Nextel requires all customers to establish and use a username and passcode. Prior to establishing an online username and passcode, Sprint Nextel authenticates these customers through secure third party verification systems or by sending a temporary verification code to the customer's wireless device or by requiring the customer to input his/her UBP PIN. If the customer cannot recall his/her online username or passcode, Sprint Nextel makes several backup methods available so that those customers can retrieve that information in a secure manner.

Sprint Nextel has developed compliant processes to handle wireline customers who contact Sprint Nextel via telephone. If a wireline customer requests access to his/her call detail records, Sprint Nextel will only send those records to the address confirmed with the customer via a follow-up outbound call to the customer's telephone number of record. Sprint Nextel also is completing development of systems to address the new CPNI requirements for its online wireline customers. The new system requirements will provide compliant solutions for the authentication of wireline customers establishing a new online account. These features impact a small segment of all wireline customers and, as stated in the Waiver Petition, Sprint Nextel expects to come into full compliance in June of 2008.

Notifications

As required by the new CPNI rules, Sprint Nextel provides notice to its customers when a triggering event occurs. Such events include the creation of, or change to, an account PIN, passcode, security question or answer, online account or address of record. These notifications are provided to customers through a variety of means, including messages via the customer's telephone number of record, postal mail or electronic mail to the customer's address of record, and text messages. The notification includes information to alert the customer of the underlying event, but does not disclose any of the new or changed information, in accordance with the FCC's rules. Consistent with Sprint Nextel's authentication obligations, the Waiver Petition addresses how Sprint Nextel is meeting notification requirements during the conversion of wireless customers to UBP and, for the small segment of impacted online wireline customers, during the completion of notification enhancements.

In the event that a breach of customer information includes CPNI, Sprint Nextel provides notice to impacted customers and law enforcement. Such notification provides customers with enough information to understand the nature of the breach, the scope of impacted information and recommendations on how the customer should respond. If the impacted customer alerts Sprint Nextel of a potential breach, Sprint Nextel will investigate the customer's allegations and communicate as necessary with the customer or government.

Data Brokers

In 2006, Sprint Nextel took vigorous action against the pretexting activities of certain unscrupulous data brokers, including the filing of lawsuits against three data brokers who fraudulently obtained and sold confidential customer information. Sprint Nextel also sent scores of cease & desist letters to data brokers believed to be engaged in or associated with pretexting activity last year.

In 2007, Sprint Nextel actively supported the Federal Trade Commission's (FTC) investigation of, and lawsuit against, a data broker. On April 26, 2006, the FTC filed suit against Accusearch, Inc., for violation of Section 5(a) of the FTC Act[6] and 15 U.S.C. § 45(a). The FTC asserted that Accusearch was illegally obtaining and selling call detail records. Kent Nakamura, Sprint Nextel's Vice President and Chief Privacy Officer, served as a witness for the FTC. With help from Mr. Nakamura and others, the FTC was able to build its case against Accusearch. The FTC's request for relief was granted in late December of 2007 and Accusearch was permanently restrained and enjoined from obtaining, marketing, or selling customer phone records and consumer personal information that is derived from customer phone records without proper authorization and consent. Accusearch was also ordered to pay a fine. The FTC publicly thanked Sprint Nextel, among others, for their assistance in this lawsuit. Accusearch has appealed the decision to the United States Court of Appeals for the Tenth Circuit.

CPNI Complaint Reporting

In response to the new CPNI complaint reporting requirements, Sprint Nextel's fraud team, which handles the complaint documentation and reporting processes, follows procedures developed in conjunction with the Legal Department's Office of Privacy. These processes enable Sprint to comply with the documentation and reporting obligations in the new CPNI rules, including maintaining a record of notifications to, and responses from, law enforcement and customers, and the relevant dates and descriptions of the complaints. These records are maintained for a minimum of two years.

Prior to the effective date of the new CPNI rules, Sprint Nextel did not track complaints related to unauthorized access to CPNI. Thus, the following data is comprised of all complaints related to unauthorized access received by Sprint Nextel since the effective date of the new CPNI rules. In the period between December 8th and December 31st of 2007, Sprint Nextel received 203 complaints related to unauthorized access. Some of these complaints were submitted to Sprint Nextel directly from the complainants themselves, and some have been called to Sprint Nextel's attention by government agencies or the Better Business Bureau. Sprint Nextel encountered several instances where it was not clear whether the type of incident would be considered a complaint under the CPNI rules. Many of these fraud related instances involve equipment theft rather than CPNI access. Sprint Nextel decided, in an abundance of caution, to comply with its CPNI reporting obligations by including these instances of fraud as CPNI complaints.

Most of Sprint Nextel's 2007 non-fraud related investigations revealed that complaints were connected to domestic disputes where a family member or close friend impersonates the customer and gains access to the customer's account. A review of the fraud-related cases suggests that access to CPNI is not the primary objective; rather it is likely incidental to other disputes. Sprint Nextel will continue to monitor these occurrences and make changes where necessary.

[6] 15 U.S.C. §§ 41-58, as amended.

The complaints are broken down by category, as follows:

- Number of complaints, where unauthorized access to CPNI was the primary objective of the a pretexter whom the customer knew: 6.
- Number of complaints, where unauthorized access to CPNI was the primary objective of a pretexter whom the customer did not know: 5.
- Number of complaints of a Sprint employee's or contractor's improper access: 1.
- Number of complaints of fraud-related incidents where equipment theft, rather than CPNI access, is the primary objective: 191.

Waiver Petition

On December 3, 2007, the Sprint Nextel requested that the Commission grant it a waiver of the obligations imposed on the Company pursuant to Commission Rules 64.2010 (b), (c), (e) and (f)[7] that were adopted in the *CPNI Report and Order*. A waiver is necessary to allow Sprint Nextel to finish pursuing its systematic solution for CPNI compliance through the continuing migration of its wireless customers to a new high-tech state-of-the-art billing platform-the Unified Billing Platform ("UBP")-that automates CPNI compliance through passcode verification, auto-generated customer notifications, and technical security measures. The Company designed, tested, and installed the CPNI compliant UBP. The Company also migrated millions of wireless customers on to the CPNI compliant UBP. Nonetheless, a limited waiver for a short period of time is needed while Sprint Nextel completes an orderly migration of the remaining wireless customers to the UBP. In addition, Sprint Nextel needs to complete deployment of CPNI compliant solutions for authentication of new residential and business wireline customers when first registering for an online account; and, for notification of account changes for residential and business wireline customers that have online accounts. Sprint Nextel is committed to completing both efforts by June 2008, at which time it expects to be fully compliant with the new CPNI rules.

At the time this certification is filed, the FCC has not yet acted on the Waiver Petition.

[7] 47 C.F.R. §§ 64.2010 (b), (c), (e) and (f).